This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of
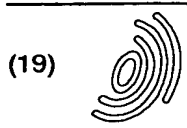the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS

- TEXT CUT OFF AT TOP, BOTTOM OR SIDES

- FADED TEXT

- ILLEGIBLE TEXT

- SKEWED/SLANTED IMAGES

- COLORED PHOTOS

- BLACK OR VERY BLACK AND WHITE DARK PHOTOS

- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.

(54) Updating domains in a postage evidencing system

(57) A postage evidencing system including a plurality of domains for partitioning a population of postage meters according to an operating characteristic, a data center, a postage meter in operative communication with the data center and a printer in operative communication with the postage meter. The postage meter is initialized to operate in a particular domain while the printer is capable of operating in each of the plurality of domains. To update or enable a domain in the printer, the postage meter transmits an indication of the particular domain to the data center. Then, the data center encrypts the indication and transmits the indication to the postage meter which in turn forwards the encrypted indication to the printer. The printer decrypts the encrypted indication and using the indication enables a respective domain in the printer corresponding to the particular domain of the postage meter. A method for updating domains in a postage evidencing system is also provided.

FIG. 1

Description

This application is related to our (ref: E612) copending European Patent Application Serial No. _____, filed concurrently herewith, and entitled SYNCHRONIZATION OF CRYPTOGRAPHIC KEYS BETWEEN TWO MODULES OF A DISTRIBUTED SYSTEM.

This invention relates to value dispensing systems. More particularly, this invention is directed to a postage evidencing system comprising a mailing machine base, a secure accounting meter detachably mounted to the base and a printer also detachably mounted to the base wherein the meter and the printer are manufactured to be interchangeable while still providing for secure mutual authentication.

One example of a value printing system is a postage evidencing system including an electronic postage meter and a printer for printing a postal indicia on an envelope or other mailpiece. Electronic postage meters for dispensing postage and accounting for the amount of postage used are well known in the art. The meter supplies evidence of the postage dispensed by printing indicia which indicates the value of the postage on an envelope or the like. The typical postage meter stores accounting information concerning its usage in a variety of registers. An ascending register tracks the total amount of postage dispensed by the meter over its lifetime. That is, the ascending register is incremented by the amount of postage dispensed after each transaction. A descending register tracks the amount of postage available for use. Thus, the descending register is decremented by the amount of postage dispensed after each transaction. When the descending register has been decremented to some value insufficient for dispensing postage, then the postage meter inhibits further printing of indicia until the descending register is resupplied with funds.

Traditionally, the postage meter and the printer have been located within a single secure housing. Examples of this type of postage evidencing system are the PostPerfect™ and Personal Post Office™ available from Pitney Bowes, Inc. of Stamford, Connecticut, USA. In this environment, the communications between the postage meter and the printer may be either secure or nonsecure. However, recently efforts have been undertaken to provide a postage meter and a printer which are physically separated from each other. Thus, in this type of postage evidencing system, the postage meter and the printer are no longer contained within the same secure housing and the communication lines between the postage meter and the printer are generally nonsecure.

Using nonsecure communication lines between the postage meter and the printer creates a risk of loss of postal funds through fraud. For example, when data necessary to print a valid postal indicia is transferred over the nonsecure communication lines from the post-

age meter to the printer, it is susceptible to interception, capture and analysis. If this occurs, then the data may be retransmitted at a latter time back to the printer in an attempt to fool the printer into believing that it is communicating with a valid postage meter. If successful, the result would be a fraudulent postage indicia printed on a mailpiece without the postage meter accounting for the value of the postage indicia.

Generally, it is known to employ secret cryptographic keys in postage evidencing systems to prevent such fraudulent practices. This is accomplished by having the postage meter and the printer authenticate each other prior to any printing taking place. One such system is described in European Patent Application Serial No. 0782111, filed on December 20, 1996, and entitled METHOD AND APPARATUS FOR SECURELY AUTHORIZING PERFORMANCE OF A FUNCTION IN A DISTRIBUTED SYSTEM SUCH AS A POSTAGE METER. In summary, this application provides a postage evidencing system including a meter and a printer each having an identical set of authentication keys stored in their respective memories. On a random basis, the printer and the meter in secret fashion coordinate the selection of which authentication key will be used to perform mutual authentication. Importantly, if a valid mutual authentication is to be obtained, it is necessary that the same key is selected for use by the meter and the printer.

Although this system generally works well, it suffers from certain disadvantages and drawbacks. For example, the set of authentication keys are the same for every postage evidencing system. That is, the set of authentication keys are universal in that they will operate with any postage evidencing system. Thus, if one postage evidencing system is compromised, then the other postage evidencing systems are also compromised.

To address this problem, other prior art postage evidencing systems have proposed a different system which provides a unique set of authentication keys for each postage meter and printer combination. In this arrangement, if one postage evidencing system is compromised, then the other postage evidencing systems are not compromised. However, the postage meter and the printer are dedicated to each other because each particular postage meter is tied to only one printer, and vice versa. Thus, interchangeability of components, such as using the same postage meter with a plurality of different printers or replacing a defective printer in the postage evidencing system, is difficult due to the necessity of reconfiguring the meter and the printer to each other. This would require updating of the authentication key sets which would increase costs and operating expenses.

Therefore, there is a need for a postage evidencing system that reduces the exposure of universal keys and allows for the interchangeability of postage meters with printers.

Accordingly, it is an object of the present invention to provide a postage evidencing system with improved security and interchangeability which substantially overcomes the problems associated with the prior art.

In accomplishing this and other objects there is provided a postage evidencing system including a plurality of domains for partitioning a population of postage meters according to an operating characteristic, a data center, a postage meter in operative communication with the data center and a printer in operative communication with the postage meter. The postage meter is initialized to operate in a particular domain while the printer is capable of operating in each of the plurality of domains. To update or enable a domain in the printer, the postage meter transmits an indication of the particular domain to the data center. Then, the data center encrypts the indication and transmits the indication to the postage meter which in turn forwards the encrypted indication to the printer. The printer decrypts the encrypted indication and using the indication enables a respective domain in the printer corresponding to the particular domain of the postage meter.

In accomplishing this and other objects there is provided a corresponding method for updating the domains in a postage evidencing system.

Therefore, it should now be apparent that the invention substantially achieves all the above objects and advantages. Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. Moreover, the objects and advantages of the invention may be realized and obtained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate presently preferred embodiments of the invention, and together with the general description given above and the detailed description of the preferred embodiments given below, serve to explain the principles of the invention. As shown through out the drawings, like reference numerals designate like or corresponding parts.

Fig. 1 is a schematic representation of a postage evidencing system including a postage meter and a printer in accordance with the present invention.

Fig. 2 is a table showing a complete set of printer specific keys, one for every domain, which have been loaded into a memory of the printer during manufacture in accordance with the present invention.

Fig. 3 is a flow chart showing a routine to synchronize the printer with the postage meter in the field in accordance with the present invention.

Fig. 4 is a flow chart showing a routine to add a domain to the printer in the field in accordance with the present invention.

Fig. 5 is a flow chart showing a routine to derive a key necessary to synchronize the printer with the postage meter in the field in accordance with the present invention.

Fig. 6 is a flow chart showing a routine to mutually authenticate a communication session between the printer and the postage meter prior to printing postal indicia in accordance with the present invention.

Referring to Fig. 1, a postage evidencing system 100 in accordance with a first embodiment of the invention is shown. The postage evidencing system 100 includes a mailing machine base 110, a postage meter 120 and a printer 130.

The mailing machine base 110 includes a variety of different modules (not shown) where each module performs a different task on a mailpiece (not shown), such as: singulating (separating the mailpieces one at a time from a stack of mailpieces), weighing, moistening/sealing (wetting and closing the glued flap of an envelope) and transporting the mailpiece through the modules. However, the exact configuration of each mailing machine is particular to the needs of the user. Additionally, the mailing machine base 110 includes an interface (not shown) of any conventional design, such as an LCD display and keypad, for communicating information to the user and receiving inputs from the user. The mailing machine base 110 further includes a controller 112 which oversees the operation of all the modules of the mailing machine base 110. Since a detailed description of the mailing machine base 100 is not necessary for an understanding of the present invention, its description will be limited for the sake of conciseness.

The postage meter 120 is detachably mounted to the mailing machine base 110 by any conventional structure (not shown) and includes a controller 122 having a memory 124, a security application specific integrated circuit (ASIC) 126 having suitable memory and logic (not shown) and a microprocessor 128. The controller 122 is in operative communication with the controller 112 of the mailing machine base 110 over suitable communication lines. Additionally, the controller 122 of the postage meter 120 is in operative communication with a remote data center 10 over suitable communication lines, such as a telephone line 20. The data center 10 communicates with the postage meter 120 for the purposes of remote inspection of accounting registers (not shown), downloading of postal funds and other purposes described in more detail below.

The printer 130 is also detachably mounted to the mailing machine base 110 by any conventional structure (not shown) and includes a print mechanism 136 and controller 132 having a memory 134 and a microprocessor 138. Alternatively, the memory 134 could be located within the microprocessor 138. The controller 132 is in operative communication with the controller 122 of the postage meter 120 and the print mechanism

136 over suitable communication lines. The print mechanism 136 prints a postal indicia (not shown) on the mailpiece (not shown) in response to instructions from the postage meter 120 which accounts for the value of the postage dispensed in conventional fashion. The print mechanism 136 may be of any suitable design, such as: rotary drum, flat impression die, thermal transfer, ink jet, xerographic or the like.

To provide for security of postal funds and to prevent fraud, the postage meter 120 and the printer 130 are provided with secret cryptographic keys which are necessary for mutual authentication. Stored within the memory 124, preferably of the non-volatile type, of the postage meter 120 is a print head/meter universal key $K_{phm}x$. To limit exposure of the universal key $K_{phm}x$ to being compromised, the world is geographically split into multiple domains each with its own separate universal key $K_{phm}x$. In the preferred embodiment, the world is divided into thirteen (13) domains. Thus, a unique universal key $K_{phm}x$ exists for each domain. For example, a unique universal key $K_{phm}1$ is provided for domain #1, a unique universal key $K_{phm}2$ is provided for domain #2, and so on. However, only one universal key $K_{phm}x$ is provided in each postage meter 120 depending upon the domain in which the postage meter 120 is authorized for use by the local postal authority. Therefore, if the first domain universal key $K_{phm}1$ is compromised, then postage meters 120 in domain #2 through domain #13 will not be compromised. Additionally, a test domain used for diagnostics and manufacturing testing is also provided having a unique universal key $K_{phm}test$.

For added security, the universal key $K_{phm}x$ is stored in memory 124 in encrypted form using an embedded security key K_{es}. Thus, the meter 120 must decrypt the universal key $K_{phm}x$ prior to use. In the preferred embodiment, the embedded security key K_{es} is only utilized for decrypting the universal key $K_{phm}x$ and is therefore distinct from the other keys used with the postage evidencing system 100. A more detailed description of this procedure is provided below.

In similar fashion, the printer 130 is also provided with secret cryptographic keys which are necessary for mutual authentication. Referring to Figs. 1 and 2, stored within the memory 134 of the printer 130 is a table 135, as shown in Fig. 2, that contains a complete set of printer specific keys $K_{ph}x$, one for every domain, which have been loaded into the printer 130 during manufacture. Thus, the set of keys $K_{ph}x$ includes $K_{ph}1$ through $K_{ph}13$ and $K_{ph}test$ which correspond to the geographic domains discussed above with respect to the postage meter 120. Also stored within the memory 134 of the printer 130 is a serial number N_{ph} which is a unique number for every printer 130. The set of keys $K_{ph}x$ are derived during manufacture by encrypting the serial number N_{ph} using the universal keys $K_{phm}x$ according to the following equation:

$$K_{ph}x = DES\ (N_{ph};\ K_{phm}x) \qquad (1)$$

where DES represents a Data Encryption Standard encryption engine, the serial number N_{ph} represents the message to be encrypted and the key $K_{phm}x$ represents the cryptographic key used to perform the encryption. Thus, a unique set of printer keys $K_{ph}x$ exists for each printer 130 which correspond to the geographic domains. For example, the key $K_{ph}1$ is unique for the printer 130 and is provided for domain #1 by deriving it from equation (1) through appropriate substitution: $K_{ph}1 = DES\ (N_{ph};\ K_{phm}1)$. The remaining keys $K_{ph}x$ are derived in similar fashion.

By providing the printer 130 with the set of printer keys $K_{ph}x$, one for every domain, it should be appreciated that the printer 130 as manufactured has the capability to operate in any domain. This is achieved by shipping the printer 130 with only the test domain enabled, as indicated in the table of Fig. 2, and then synchronizing the printer 130 with a postage meter 120 located within a particular domain in the field. This is in contrast to the meter 120 which is only provided with one universal key $K_{phm}x$ depending upon the domain where the postage meter 120 is authorized for use by a governing postal authority.

The mailing machine base controller 112, the postage meter controller 122 and the printer controller 132 all work cooperatively to execute a plurality of routines, described in detail below, in accordance with the present invention. Thus, they contain suitable software and hardware to accomplish those functions described in the routines. With respect to some functions, it is a matter of design choice where they can be implemented. With respect to other functions, it is important they be implemented in a particular controller 112, 122 or 132. This will be evident to those skilled in the art from the detailed descriptions below.

To synchronize the printer 130 with the postage meter 120 in the field, the postage evidencing system 100 executes a routine 300 as shown in Fig. 3. Referring primarily to Fig. 3 while referencing the structure of Fig. 1, at 302, the postage meter 120 and the printer 130 are powered up and each performs self diagnostics to ensure that normal operating conditions exist. At 304, a determination is made whether the domain of the meter 120 has been enabled in the printer 130. If yes, then at 306 the postage evidencing system 100 begins normal operations and proceeds to execute a key synchronization routine 500 to ensure that the meter 120 is communicating with a valid printer 130 and that the printer 130 is communication with a valid meter 120 prior to printing any postal indicia. However, if at 304 the answer is no, then at 308 a determination is made whether the test domain of the printer 130 is enabled. If yes, then at 310, the domain in the printer 130 which corresponds to the domain of the meter 120 is enabled. Then, at 312 the test domain is permanently disabled before proceeding to normal operations at 306. However, if at 308 the answer is no, then an add domain routine 400 is executed.

Referring primarily to Fig. 5 while referencing the structure of Fig. 1, a description of the key synchronization routine 500 will now be provided. At 502, the serial number N_{ph} of the printer 130 is sent to the security ASIC 126. Next, at 504 the encrypted universal key $K_{phm}x$ is brought from the memory 124 to the security ASIC 126. Next, at 506 the encrypted universal key $K_{phm}x$ is decrypted using the security key K_{es} which is embedded within the security ASIC 126. Thus, the security key K_{es} is masked within the hardware of the security ASIC 126 and generally not discernible to the outside world. Next, at 508 key $K_{ph}x$ is derived within the security ASIC 126 using equation (1). It should now be apparent to those skilled in the art that keys have been synchronized between the meter 120 and the printer 130 without transmitting the keys themselves. Furthermore, the keys used are unique to that meter 120 and printer 130 combination only. That is, since the serial number N_{ph} of the printer 130 is unique to each printer 130 in the preferred embodiment so as to provide the greatest degree of security, no two keys $K_{ph}x$ are the same. In summary, the meter 130 has the capability to make a key $K_{ph}x$ which is specific to the particular printer 130 with which it is in communication. Therefore, the interchangeability of the meters 120 with the printers 130 is provided for. Once the keys have been synchronized, the postage evidencing system 100 then proceeds to execute a mutual session authentication routine 600.

It should now be apparent to those skilled in the art that the present invention provides for secure communications and interchangeability between the postage meter 120 and the printer 130. For example, if the printer 130 become defective and needs to be replaced in the field, then a new printer 130 could be shipped and installed by a service person without regard to the domain that the new printer 130 is being shipped into or the particular meter 120 that the new printer 130 will be interfaced to. This is because upon the first communication between the meter 120 and the printer 130, the meter 120 will derive the appropriate key $K_{ph}x$ which is particular to the new printer 130 and enable the appropriate domain in the new printer 130. As another example, if a new meter 120 is installed for use with the existing printer 130, then the new meter will also derive the appropriate key $K_{ph}x$ which is particular to the existing printer 130 just as the replaced meter 120 had done.

In the preferred embodiment, it is desirable not to allow the meter 120 to change the domain which is enabled within the printer 130 other than at the time when the printer 130 is first placed into service and the domain is changed from the test domain as described above in the routine 300 in Fig. 3. Therefore, the postage evidencing system 100 must communicate securely with the remote data center 10 to obtain authorization to enable an additional domain within the printer 130. In this manner, an added level of security is achieved. Otherwise, the exposure to fraud if a universal key $K_{phm}x$

were to become compromised would be far greater. For example, if the meter 120 were permitted to change the domain of the printer 130, then a compromised universal key for domain #1 $K_{phm}1$ would lead to a greater amount of fraud. This is because the compromised universal key for domain #1 $K_{phm}1$ could be loaded into other meters 120 located outside of domain #1. Then these other meters 120, in addition to those located in domain #1, would also be able to print fraudulent postal indicias if the other meters 120 had the capability to change the domain of their associated printer 130. Therefore, the risk of fraud would greatly increase. Moreover, the manufacturer would be compelled not only to recall those printers 130 located in domain #1, but also in every other domain. This would prove to be administratively complex and costly.

Base on the above factors, the meter 120 is not allowed to change the domain of the printer 130 once the printer 130 has been initialized for the first time. Referring primarily to Fig. 4 while referencing the structure of Fig. 1, a description of the add domain routine 400 will now be provided. At 402, the user is prompted by the mailing machine base 110 to initiate communication with the data center 10 for the purpose of adding a domain to the printer 130. Next, at 404, the meter 120 initiates communication with the data center 10 via telephone line 20. Next, at 406, the meter 120 obtains the serial number N_{ph} from the printer 130 and assembles a first message which includes the serial number N_{ph}, a meter serial number N_m which is a unique number for each meter 120 and the domain number. This first message is transmitted to the data center 10 by the meter 120. Next, at 408, the data center 10 makes a determination whether the meter 120 is valid. This involves: (i) looking up in a database to see if the meter serial number N_m which has been received has been placed into service and is active; and (ii) comparing the domain number in the database associated with the meter serial number N_m with the domain number which has been received to see if they match. To be valid, the meter 120 must survive both inquiries. If at 408 the answer is no, then at 410 a failure occurs and the user is instructed to contact the data center 10 before power resetting the postage evidencing device 100. On the other hand, if at 408 that answer is yes, then at 412 the data center transmits a second message to the meter 120 which includes the serial number N_{ph} and the domain number. This second message is encrypted using a remote communications key K_d stored in the data center 10. In the preferred embodiment, the remote communications key K_d is only utilized for remote communications and is therefore distinct from the other keys used with the postage evidencing system 100. That is, there is no overlap between the remote communications key K_d, the security key K_{es}, the universal keys $K_{phm}x$ and the printer keys $K_{ph}x$. At 414, the meter 120 forwards the second message to the printer 130. Next, at 416, the printer 130 decrypts the second message using the same key K_d

stored in the memory 134 of the printer 130 and makes a determination whether the received serial number N_{ph} matches the actual serial number N_{ph} of the printer 130. If no, then the routine 400 proceeds to 410 where a failure results. If yes, then at 418 the domain corresponding to the received domain number is enabled. Next, the routine 400 proceeds to 306 and operation continues accordingly. In the preferred embodiment, domains are never disabled (except for the test domain). Thus, the domain that is enabled according to the routine 400 is in addition to any other domains which have been previously enabled. Thus, the table 135 as shown in Fig. 2 will be updated accordingly with an "Enable" in the second column indicating that the domain is enabled and a "Disable" indicating those domains that are not enabled.

Referring primarily to Fig. 6 while referencing the structure of Fig. 1, a description of the mutual session authentication routine 600 will now be provided. To ensure that postal funds are appropriately accounted for and that fraudulent postal indicias are not produced, the postage meter 120 and the printer 130 initiate the mutual authentication routine 600 prior to any printing taking place. At 602, the controller 112 of the mailing machine base 110 sends an initialize session signal to the meter 120 in response to the occurrence of one of a plurality of predetermined events, such as: the start of a batch run of envelopes or after a predetermined number (for example, 200) of envelopes within the batch run. Next, at 604 the meter forwards the initialize session signal to the printer 130. Next, at 606 the printer 130 generates a first session nonce SN_p which is a random number generated in software in the printer controller 132. Next, at 608 the printer 130 sends the first session nonce SN_p to the meter 120. Next, at 610 the meter 120 derives a session key K_s according to the equation:

$$Ks = DES\ (SN_p;\ K_{ph}x) \qquad (2)$$

where DES represents the Data Encryption Standard encryption engine, the first session nonce SN_p represents the message to be encrypted using the key $K_{ph}x$ which is the synchronized key obtained as described above. Next, at 612 the meter 120 generates a second session nonce SN_m which is a random number generated in the meter controller 122. Next, at 614 the meter encrypts the first session nonce SN_p and the second session nonce SN_m using the key Ks and sends the resulting message to the printer 130. Next, at 616 the printer 130 derives the session key K_s independently from the meter 120 using equation (2). Next, at 618 the printer 130 decrypts the encrypted message sent from the meter 120 using the key Ks. Next, at 620 the printer 130 makes a determination whether the decrypted first session nonce SN_p that was received and the first session nonce SN_p that was sent match. If no, then at 622 a failure results and printing is disabled and the user is instructed to power reset the postage evidencing system 100. If yes, then at 624 the printer concludes that the meter 120 is valid. Next, at 626 the printer 130 sends the decrypted second session nonce SN_m to the meter 120. Next, at 628 the meter 120 makes a determination whether the decrypted second session nonce SN_m that was received and the second session nonce SN_m that was sent match. If no, then the routine proceeds to 622 indicating a failure has occurred. If yes, then at 630 the meter 120 concludes that the printer 130 is valid. Next, since the meter 120 and the printer 130 have successfully authenticated each other, at 632 the postage evidencing system 100 is to print a postal indicia and account for the postage dispensed. Generally, this is accomplished in a conventional manner by generating a secure token in the meter 120 which contains information necessary to print the postal indicia and communicating that token to the printer 130. Since this procedure is not necessary for an understanding of the present invention, no further description will be provided.

Those skilled in the art will now appreciate that since the set of printer keys $K_{ph}x$ are unique to each printer 130 and each respective domain, a high degree of security is maintained. For example, if key $K_{ph}1$ is compromised for a particular printer 130, then the security breach is confined to that particular printer 130 in the domain in which it is operating. Thus, the printers 130 and the postage meters 120 operating in the same domain and in other domains are not compromised.

Many features of the preferred embodiment represent design choices selected to best exploit the inventive concept as implemented in a postage evidencing device. However, those skilled in the art will recognize that various modifications can be made without departing from the spirit of the present invention. For example, the domains could be partitioned in a number of different manners, such as: by customer, by country, by customer and by country or any other predetermined segmentation that makes sense given the particular application. As another example, the placement of the universal key could be in the printer while the specific or unique keys were in the meter. In other words, a reversal of the operating relationship described above. As still another example, another encryption engine other than DES, such as RSA, could be substituted.

As yet another example, those skilled in the art will recognize that the mailing machine base controller 112, the meter controller 122 and the printer controller 132 can be of any conventional design incorporating appropriate hardware and software. As still another example, those skilled in the art will recognized that the routine 400 could be utilized to not only enable subsequent domains but also the first domain when the printer 130 is first initialized by a meter 120.

Therefore, the inventive concept in its broader aspects is not limited to the specific details of the preferred embodiment but is defined by the appended claims and their equivalents.

Claims

1. A postage evidencing system, comprising:

   a plurality of domains for partitioning a population of postage meters according to an operating characteristic;
   a data center;
   a postage meter in operative communication with the data center, the postage meter initialized to operate in a particular domain; and
   a printer in operative communication with the postage meter, the printer capable of operating in each of the plurality of domains; and
   wherein:
   the postage meter transmits an indication of the particular domain to the data center;
   the data center encrypts the indication and transmits the indication to the postage meter;
   the postage meter transmits the encrypted indication to the printer;
   the printer decrypts the encrypted indication and using the indication enables a respective domain in the printer corresponding to the particular domain of the postage meter.

2. The postage evidencing system of claim 1, wherein:

   the postage meter transmits an identifier uniquely associated with the postage meter to the data center; and
   using the postage meter unique identifier, the data center verifies that the postage meter is a valid postage meter before transmitting the encrypted indication to the postage meter.

3. The postage evidencing system of claim 2, wherein:

   the printer transmits an identifier uniquely associated with the printer to the postage meter;
   the postage meter transmits the printer unique identifier to the data center;
   the data center encrypts the printer unique identifier and transmits the printer unique identifier to the postage meter;
   the postage meter transmits the encrypted printer unique identifier to the printer;
   the printer decrypts the encrypted printer unique identifier and compares the printer unique identifier which the printer transmitted to the printer unique identifier which the printer received to determine if there is a match before enabling the respective domain in the printer corresponding to the particular domain of the postage meter.

4. A method of updating domains in a postage evidencing system including a data center, a postage meter in operative communication with the data center and a printer in operative communication with the postage meter, the method comprising the step(s) of:

   establishing a plurality of domains for partitioning a population of postage meters according to an operating characteristic;
   initializing a postage meter to operate in a particular domain;
   providing the printer with capability to operate in each of the plurality of domains;
   transmiting an indication of the particular domain to the data center;
   encrypting the indication at the data center;
   transmiting the encrypted indication to the printer;
   decrypting the encrypted indication at the printer; and
   using the indication to enable a respective domain in the printer corresponding to the particular domain of the postage meter.

5. The method of claim 4, comprising the step(s) of:

   transmiting an identifier uniquely associated with the postage meter from the postage meter to the data center; and
   using the postage meter unique identifier, verifying at the data center that the postage meter is a valid postage meter before transmitting the encrypted indication to the postage meter.

6. The method of claim 5, comprising the step(s) of:

   transmitting an identifier uniquely associated with the printer from the printer to data center via the postage meter;
   encrypting the printer unique identifier at the data center;
   transmiting encrypted the printer unique identifier to printer via the postage meter; and
   decrypting the encrypted printer unique identifier at the printer and comparing the printer unique identifier which the printer transmitted to the printer unique identifier which the printer received to determine if there is a match before enabling the respective domain in the printer corresponding to the particular domain of the postage meter.
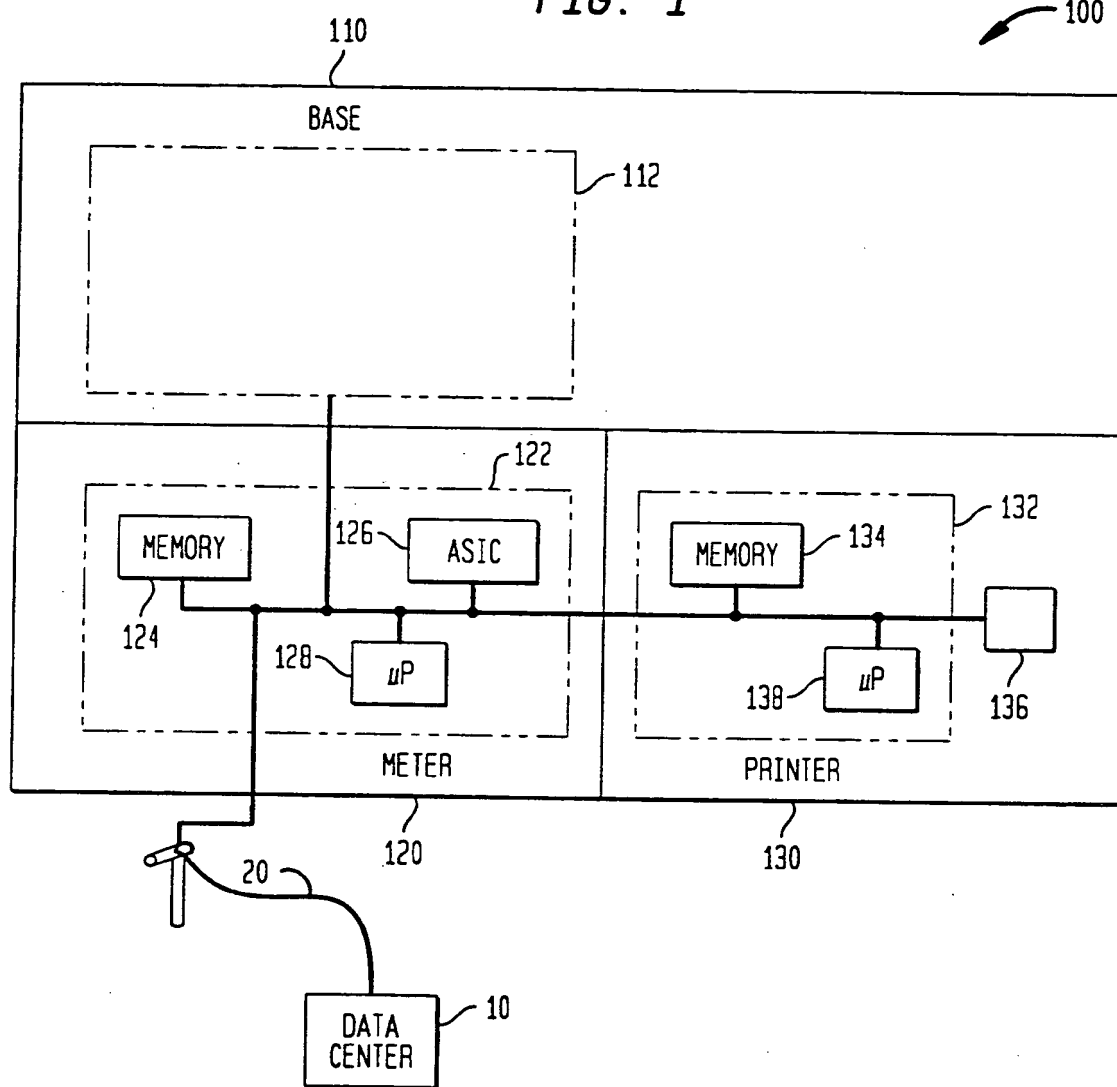
FIG. 1

100

110

BASE

112

122

| MEMORY | | ASIC | | | MEMORY | |
124 126 134 132

128 μP 138 μP

136

METER 120

PRINTER 130

DATA
CENTER 10

20

FIG. 2

135

DOMAIN	ENABLE	KEY
1	0	$K_{phm}1$
2	0	$K_{phm}2$
3	0	$K_{phm}3$
4	0	$K_{phm}4$
5	0	$K_{phm}5$
6	0	$K_{phm}6$
7	0	$K_{phm}7$
8	0	$K_{phm}8$
9	0	$K_{phm}9$
10	0	$K_{phm}10$
11	0	$K_{phm}11$
12	0	$K_{phm}12$
13	0	$K_{phm}13$
TEST	1	$K_{phm}test$
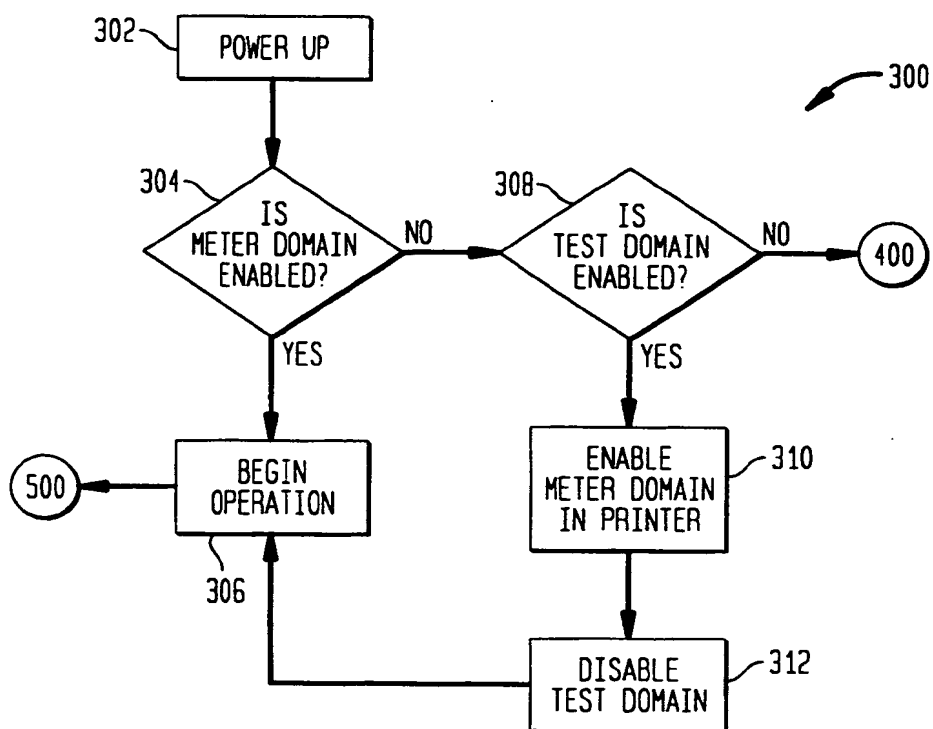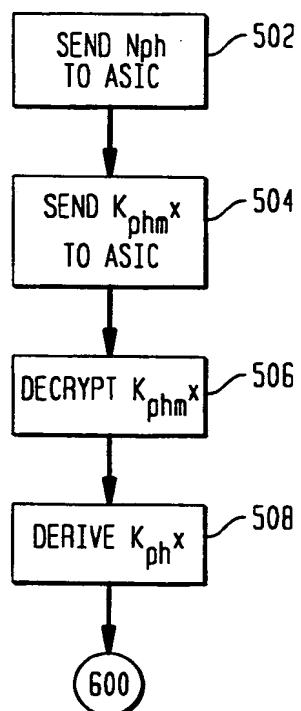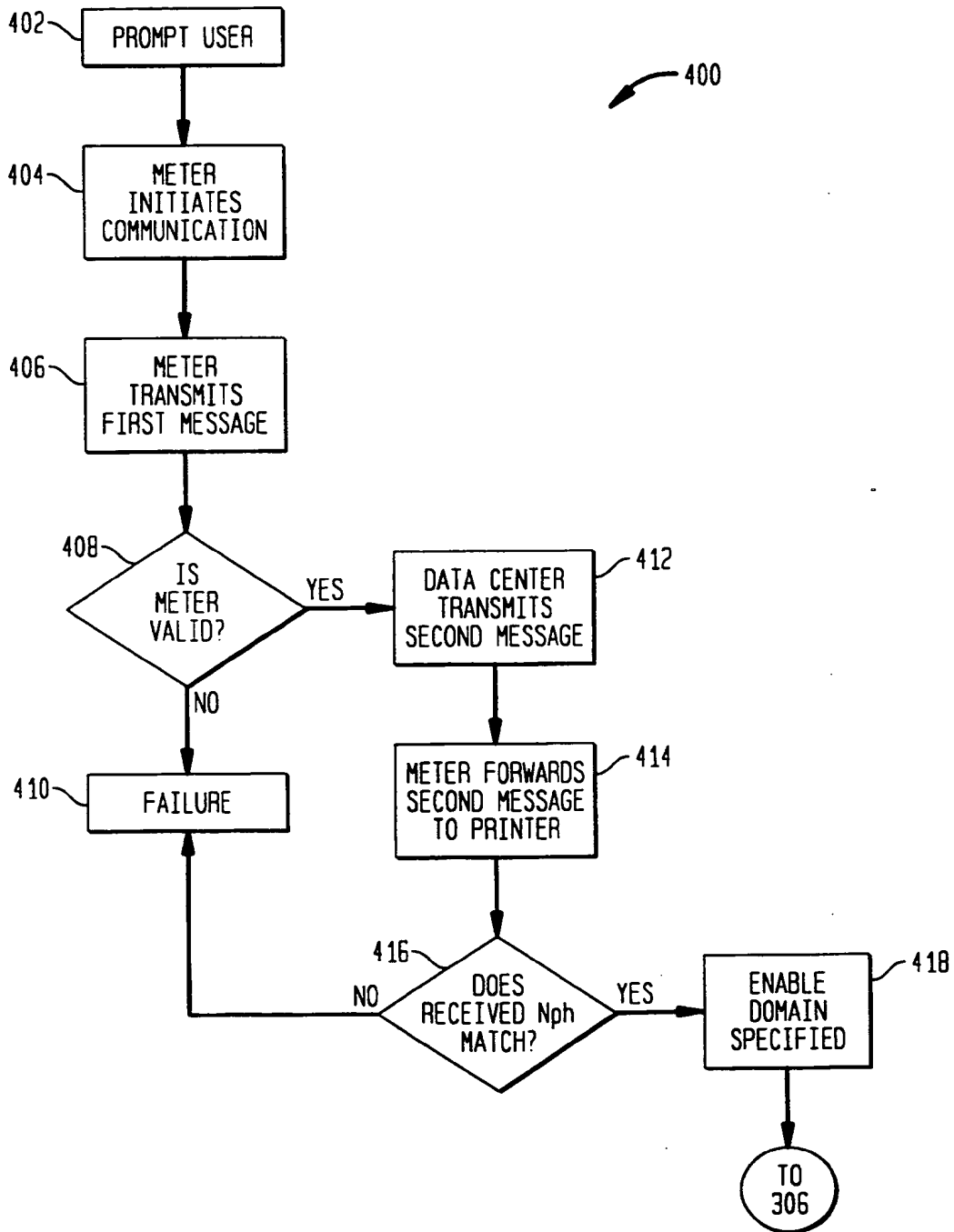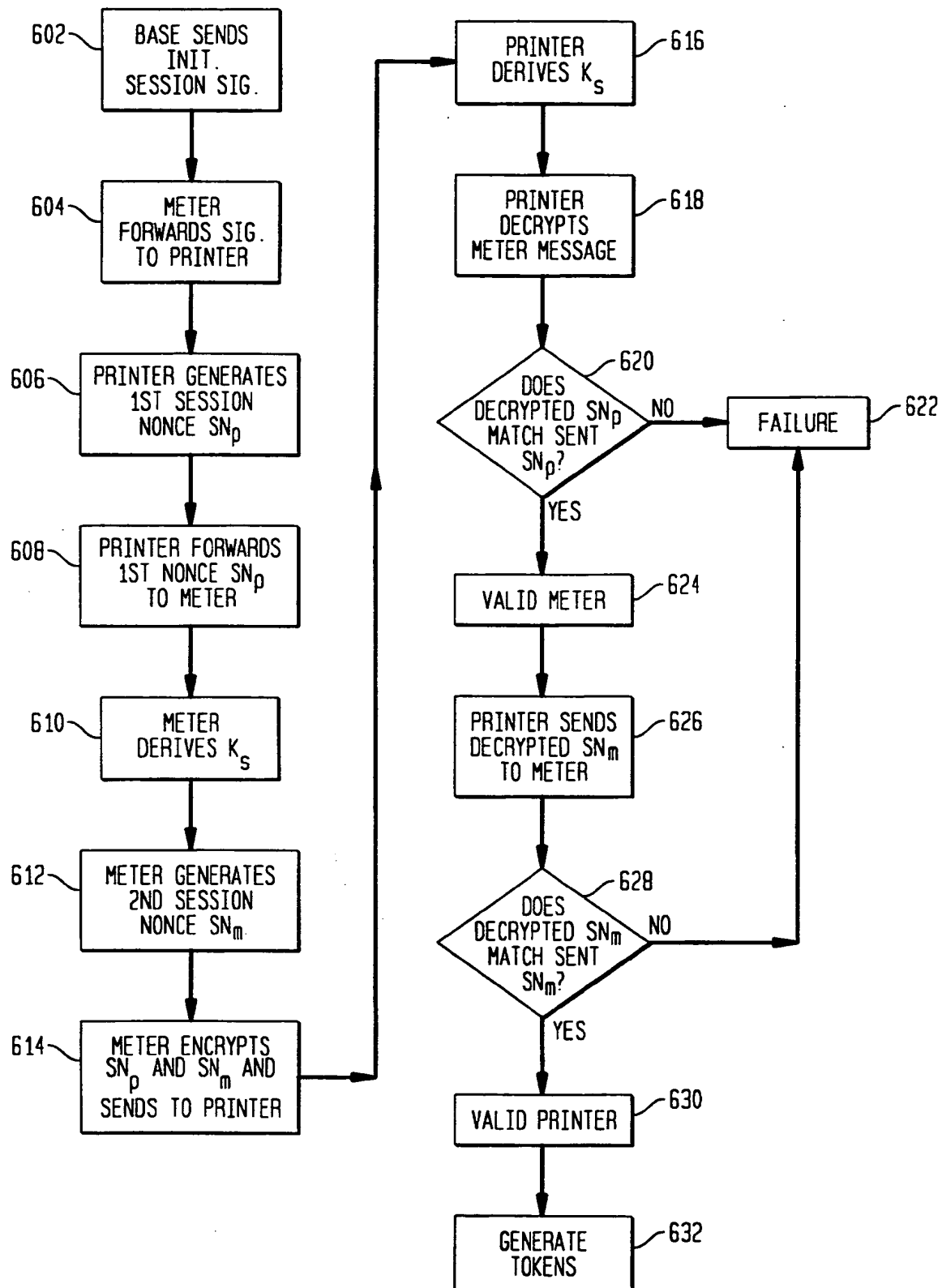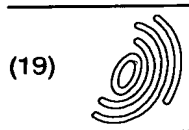
9

FIG. 3

302 — POWER UP

300

304 — IS METER DOMAIN ENABLED? — NO → 308 — IS TEST DOMAIN ENABLED? — NO → (400)

YES ↓ (304)

YES ↓ (308)

(500) ← BEGIN OPERATION

306

ENABLE METER DOMAIN IN PRINTER — 310

DISABLE TEST DOMAIN — 312

FIG. 5

500

SEND Nph TO ASIC — 502

SEND $K_{phm}x$ TO ASIC — 504

DECRYPT $K_{phm}x$ — 506

DERIVE $K_{ph}x$ — 508

(600)

10

FIG. 4

402 — PROMPT USER

— 400

404 — METER INITIATES COMMUNICATION

406 — METER TRANSMITS FIRST MESSAGE

408 — IS METER VALID?

YES → DATA CENTER TRANSMITS SECOND MESSAGE — 412

NO

410 — FAILURE

METER FORWARDS SECOND MESSAGE TO PRINTER — 414

416 — DOES RECEIVED Nph MATCH?

NO

YES → ENABLE DOMAIN SPECIFIED — 418

TO 306

FIG. 6

600

602 — BASE SENDS INIT. SESSION SIG.

604 — METER FORWARDS SIG. TO PRINTER

606 — PRINTER GENERATES 1ST SESSION NONCE SN_p

608 — PRINTER FORWARDS 1ST NONCE SN_p TO METER

610 — METER DERIVES K_s

612 — METER GENERATES 2ND SESSION NONCE SN_m

614 — METER ENCRYPTS SN_p AND SN_m AND SENDS TO PRINTER

616 — PRINTER DERIVES K_s

618 — PRINTER DECRYPTS METER MESSAGE

620 — DOES DECRYPTED SN_p MATCH SENT SN_p?

NO → FAILURE — 622

YES

624 — VALID METER

626 — PRINTER SENDS DECRYPTED SN_m TO METER

628 — DOES DECRYPTED SN_m MATCH SENT SN_m?

NO

YES

630 — VALID PRINTER

632 — GENERATE TOKENS

(71) Applicant: PITNEY BOWES INC.
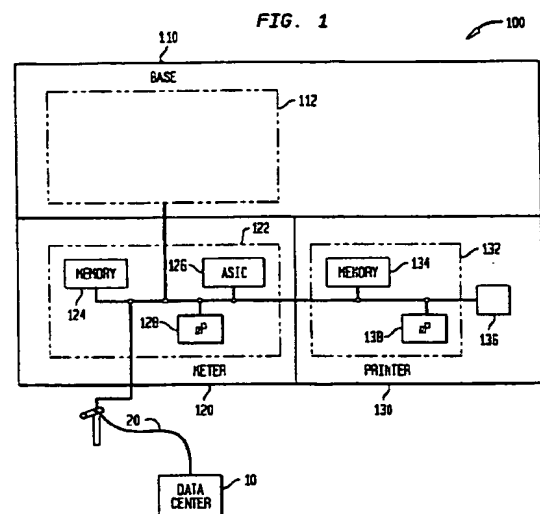Stamford, Connecticut 06926-0700 (US)

(72) Inventors:
 • Cordery, Robert A.
  Danbury, CT 06811 (US)
 • Davies, Brad L.
  Trumbull, CT 06611 (US)

 • Loglisci, Louis J.
  Stamford, CT 06902 (US)
 • Parkos, Maria P.
  Southbury, CT 06478 (US)
 • Ryan, Frederick W., Jr.
  Oxford, CT 06478 (US)
 • Scribe, Mark A.
  Southbury, CT 06478 (US)
 • Steinmetz, John H.
  Bridgeport, CT 06606 (US)

(74) Representative:
Avery, Stephen John et al
Hoffmann Eitle,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Updating domains in a postage evidencing system

(57) A postage evidencing system including a plurality of domains for partitioning a population of postage meters according to an operating characteristic, a data center, a postage meter in operative communication with the data center and a printer in operative communication with the postage meter. The postage meter is initialized to operate in a particular domain while the printer is capable of operating in each of the plurality of domains. To update or enable a domain in the printer, the postage meter transmits an indication of the particular domain to the data center. Then, the data center encrypts the indication and transmits the indication to the postage meter which in turn forwards the encrypted indication to the printer. The printer decrypts the encrypted indication and using the indication enables a respective domain in the printer corresponding to the particular domain of the postage meter. A method for updating domains in a postage evidencing system is also provided.

FIG. 1

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 98 10 9735

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 647 924 A (PITNEY BOWES) 12 April 1995 (1995-04-12) * column 2, line 47 - column 3, line 32 * * column 6, line 29 - line 46 * * abstract; claim 1; figure 4 *	1,2,4,5	G07B17/02
A	EP 0 735 721 A (PITNEY BOWES) 2 October 1996 (1996-10-02) * column 3, line 10 - line 59 * * column 12, line 3 - line 18 * * abstract; claims 1-3; figure 2 *	1,2,4,5	
A	EP 0 718 803 A (PITNEY BOWES) 26 June 1996 (1996-06-26) * column 1, line 37 - column 2, line 33 * * abstract; claim 1; figure 2 *	1,4	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G07B
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 April 2000	Reule, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**
EP 98 10 9735

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-04-2000

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0647924	A	12-04-1995	US	5878136 A	02-03-1999
			CA	2133679 A	09-04-1995
			EP	0942398 A	15-09-1999
EP 0735721	A	02-10-1996	US	5680456 A	21-10-1997
			BR	9601233 A	06-01-1998
			CA	2172861 A	01-10-1996
			CN	1148765 A	30-04-1997
			JP	9190555 A	22-07-1997
EP 0718803	A	26-06-1996	US	5606613 A	25-02-1997
			CA	2165102 A	23-06-1996
			CN	1131851 A	25-09-1996
			JP	8273011 A	18-10-1996

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82